Certificateless and provably-secure digital signature scheme based on elliptic curve

Dhanashree Toradmalle¹, Jayabhaskar Muthukuru², B. Sathyanarayana³
¹,²Department of CSE, KLEF, India
³Department of Computer Science and IT, Sri Krishnadevaraya University, India

ABSTRACT

With the internet today available at the user’s beck, and call data or Information Security plays a vital role. Confidentiality, Integrity, Availability, and Non-repudiation are the pillars of security on which every application on the web is based on. With these basic requirements the users also need the security in low resource constrained environments making it more challenging for the security experts to design secured cryptographic algorithms. Digital Signatures play a pivotal role in Authentication. They help in verifying the integrity of the data being exchanged. Elliptical curves are the strongest contenders in Digital Signatures, and much research is being done to enhance the method in many ways. The paper briefs a secured and improved ECDSA Elliptical Curve Digital Signature Algorithm which is an improved and secured version of the Digital Signature Algorithm.

Keywords:
Digital signature
Elliptic curve
Elliptic curve digital signature algorithm
Forward secrecy

Corresponding Author:
Dhanashree K Toradmalle,
Department of CSE,
Koneru Lakshmaiah Education Foundation (KLEF),
Vaddeswaram, Andhra Pradesh 522502, India.
Email: dhanashree.kt@gmail.com

1. INTRODUCTION

A digital signature [1] is a technique by which the Sender can sign an electronic report for the Verifier to keep as a confirmation that the message was to be sure sent initially from the Sender. The National Institute of Standards and Technology (NIST) have proposed Digital Signatures as standards which are worldly accepted. The primary choices available for public key systems are:

- RSA
- Diffie-Hellman (DH) or Digital Signature Algorithm
- Elliptic Curve Digital Signature Algorithm

RSA is a framework that was distributed in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers. Whitfield Diffie furthermore, Martin Hellman proposed the general population key framework presently called Diffie-Hellman Key Exchange in 1976. DH and DSA work for key agreement and Digital signature respectively and can be consolidated to do verified key agreement. They are based on the difficulty of solving the discrete logarithm problem in the multiplicative group of integers modulo a prime p. In 1985 elliptic curve groups were presented byNeal and Koblitz as an alternate for multiplicative groups modulo p. Elliptic curve based digital signatures overcame all the drawbacks of its predecessors with smaller key size thus entering the foray of applications with resource constraints. [2]. The major areas of IoT applications [3] face challenges for resource constrained applications which will surely benefit from the ECDSA based IoT applications in terms of security. The wireless sensor networks are another domain where ECC based applications are in vogue [4]
Elliptical Curve Cryptography [ECC] optimizes encryption and decryption processes of several methods. The procedure of ECC comprises of following phases [5]:
- Determining the prime points on the elliptic curve
- Forming the public and private key
- Encoding
- Encryption
- Decryption
- Decoding

Various authors have represented the elliptical curve digital signature algorithm (ECDSA) with relating equations in their literature [6-8]. They use their own conventions to present the ECDSA scheme. However, primarily ECDSA needs the accompanying significant calculations:
- Generation of a key combine (private key, public key),
- The calculation of a signature,
- And, the confirmation of the signature

There are many advantages of ECDSA over its predecessors [9]:
- More Secure
- Low computation resources
- Small key sizes

In real-time three cases occur most ordinarily inside the method of communication:
- Message has been tampered.
- The sender denies causing the message.
- The receiver faux the message.

ECDSA though is the most groundbreaking of all the asymmetric digital signature strategies, specialists are putting every one of their endeavours to make it more grounded to withstand different difficulties. Scientists have also proposed Elliptic curve Digital signature scheme based on certificates [10]. The following are the parameters to strengthen the ECDSA where research is going on:
- Forward Secrecy [11-12]:
  - Digital Signatures empower the Signer to ensure the security of messages marked in the past regardless of whether his mystery key is uncovered today.
- Attacks on Security:
  - Various attacks like forgery attack [13], replay attack [14], man in the middle attack pose a danger to security.

Attacks break the security and non-repudiation attributes of the ECDSA. Xianmin Wei et al [15], states improvements in ECC but fails to capture the security aspects in attacks by just focusing on the modular operations. Neetesh Saxena et al [9] proposes variants to ECDSA which focus on efficiency again, underestimating the attacks on security. Jie Liu and Jianhua Li [16] exhibits a cryptanalysis of Chang et al’s. Digital signature scheme, which was professed to oppose forgery attacks without utilizing any oneway hash capacity or padding any redundancy. Further they also propose improved signature plans, in which the length of the digital signature is a lot shorter. Lei Niu [17] presents progressively forgery attacks to tell unmistakably the best way to obtain the attacks. Jianhong Zhang and Shengnan Gao [18] breakdown the blind signatures and demonstrate that they are definitely not secure; finally giving a solution for the same. Xinghua Zhang [19] discusses an enhanced technique to overcome forgery attacks. Long Zhaohua et al [20] restrict the “Man-in-the-Middle” attacks but requires three entities participating in identification authentication process in the wireless network, such as Station (STA), Access Point (AP), and Authentication Server (AS) which is an overhead to the application.

2. PROPOSED ALGORITHM

The Middle Man or intruder can without a lot of stretch modify or supervene upon the message that can't be perceived by the receiver, by merely adjusting the hash value Researchers are acting on the on top of problems keeping in mind the necessities of ECDSA that are smaller key size and high security. The afore mentioned Jhong’s scheme [21] tries to attain potency by reducing the reserve standard inverse operations however it fails to attain security; because the intruder will simply alter the message and replace the present message hash value with changed hash value and thereby it fails to attain security attributes of a digital signature scheme. Dhanashree K Toradmalle et al [22] gives a point by point cryptanalysis of the Jhong's plan and shows how Jhong's technique is inclined to man in the center assault We along these lines propose a plan which guarantees that the Forward Secrecy and Intruder assaults can be taken care of and ensure a powerful ECDSA. The proposed Algorithm is stated as follows:
2.1. Key generation
Using generating point G and random integer number r the public key K is computed as follows:

a. Choose a random integer number r in interval [0, n-1].
b. Compute K = r * G
c. The key-pair combination is (r, K) where r is the Private Key and K is the Public key.

2.2. Signature generation
To sign on message m utilizing the domain parameter and Private key the accompanying advances are performed by the Signer:

a. Selects a random integer p (secret key) with 1 ≤ p ≤ n − 1.
b. Determine the value of z = H(m)
c. Determine f = ((z + p) \oplus (p + r))
d. Determine d = x-coordinate (f * G)
e. Determine s = (z * r) + f mod n. If s = 0 then return to step 1.
f. Signature for the message m is (d, s).

2.3. Signature verification
At the Receiver side the message m ought to be validated with the following steps:

a. Firstly, confirm that s is an integer in the interim [1, n − 1]
b. Compute the hash value z of the message/document m
c. W = (x1, y1) = s * G − z * K
d. v = x-coordinate(W), finally, authenticate the signature by checking whether the equivalence v = d holds.

3. RESULTS AND DISCUSSIONS
In the event if the signature for the message m is (d, s) and was genuinely generated by the authorized Sender then s = (z * r) + f mod n. The correctness of the algorithm can be tested using the following proof:

\[ W = s * G − z * K \]
\[ = ((z * r) + f) * G − z * K \]
\[ = z * r * G + f * G − z * K \]
\[ = z * K + f * G − z * K \]
\[ = f * G \]
\[ \text{x-coordinate (W)} = \text{x-coordinate (f * G)} \]
Hence, v = d

Thus, method proposed by Hong Jhong et al, is deficient in surpassing the Man in the middle attack, which is overcome by the above proposed proof.

4. CONCLUSION
The Elliptical curve digital signature is being redeveloped and increased by several researchers to create it sturdy to resist the protection loopholes. The projected technique suggests a safer and sturdy ESDSA scheme that delivers a robust ECDSA within the context of forward secrecy and attack situations

REFERENCES
Dhanashree K. Toradmalle is working as an Associate Professor in Shah & Anchor Kutchhi Engineering College, Mumbai. She is currently pursuing her Ph.D in Computer Science Engineering from K.L.E. Foundation, Guntur, Andhra Pradesh. Her research areas include Computer Networks and Security.

M. Jayabhaskar is working as an Associate Professor in K.L.E Foundation, Vaddeswaram, India. His research area includes Network Security.

B. Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985. Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri KrishnaDevaraya University, Ananthpuramu, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals.

Certificateless and provably-secure digital signature scheme... (Dhanashree K Toradmalle)